AHIC CPS Workgroup
June 2007 Public Comment Solicitation
Healthe Mid-America[i]

Introduction

We greatly appreciate the opportunity to provide the workgroup with our perspective as well as to share our "front line" experiences – thank you. The work this group is undertaking is critical to resolving issues that are key enablers for our organization and the industry in moving forward in an efficient and effective manner. Stakeholder (especially consumer) trust is truly a foundational requirement in our collective success.

Healthe Mid-America Profile Summary

As an independent, not-for-profit organization, HealtheMid-America provides secure, longitudinal health information in both consumer and provider views in order to improve the safety, quality and efficiency of healthcare. The system is available to consumer/patients and healthcare providers free of charge.

Healthe Mid-America is an operational Kansas City based health information exchange (HIE) organization, having been rolled out to over 10K users to-date. The initiative's business model is sponsored/funded by visionary and innovative area employers (currently 24), representing 100K+ covered lives, including four hospital systems. Services are provided to employees and their dependents as a component of their benefit package. Employers do not have access to the data.

The system capabilities includes both consumer/patient and healthcare provider views of longitudinal health information, e-prescribing/drug interaction checking, as well as privacy features such as consumer controlled record access settings and self-service health record access reporting.

1. Enforceable mechanisms

The CPS workgroup understands that there may be one or more appropriate mechanisms to properly enforce and ensure that confidentiality, privacy, and security requirements are met in an electronic health information exchange environment. Therefore, the workgroup is interested in comments on appropriate, effective, and feasible ways to enforce confidentiality, privacy, and security protections in this new environment. Comments will be considered by the workgroup for the purposes of developing one or more recommendations associated with the "working hypothesis" above.

Similar to other accreditation or certification bodies that provide guidance to healthcare organizations (i.e. JCAHO, NCQA), persons or entities that participate in an electronic health information exchange or network including any organization providing services need to be held at a minimum to HIPAA standards and preferably higher standards in order to build "trust" within the community that information is both secure and kept confidential. An accreditation or certification body should be created to monitor compliance as well as assist in resolving any breaches that may occur. Timeframe for accreditation would be every 2-3 years. Each person or entity that participate need to have their own review process in order to ensure ongoing compliance with the federal requirements.

In addition, a reporting process should be implemented in order to report any privacy or security breaches that occur and how they are resolved. Breaches should be classified by standardized levels of severity and guidance on investigation and resolving issues should be drafted and made available to health information exchanges to assist in responding to privacy and security breaches. This will help alleviate the volume of privacy breaches that may need to be reported and assist organizations providing standardized responses when investigating issues. For example, minor breaches may only be reported (outside of the consumer) when an accreditation or certification process occurs.

2. Relevant requirements

For a given participant's characteristics and role in an electronic health information environment, certain confidentiality, privacy, and security requirements may be more relevant than others. The CPS workgroup requests comment as to whether particular confidentiality, privacy, and security requirements equivalent to those in the HIPAA Privacy and Security Rules should or should not apply to a particular type of person or entity and why. Please identity specific section(s) of the HIPAA Privacy and Security Rules. The following examples have been developed to identify the level of detail and specificity the workgroup is seeking in a response:

In order to encourage the use of Health Information Exchanges, it is critical that the consumer is involved in the process and has reasonable controls over their information. Health Information Exchanges should provide a consumer view of their information as well as a provider view. This will allow for more consumer engagement by placing some responsibility in their hands.

160.103 Definitions- Covered Entity: Should include the term "Health Information Exchange and/or any organization providing services for a Health Information Exchange" as the 4th type of Covered Entity. (This should also be included in section 106.102 Applicability)

164.520 Notice of Privacy Practices: Should have specific requirements for any Health Information Exchange effort that mandate the posting of their Notice of Privacy Practices on their website only. Any updates should be also easily identified on the website but providing hard copies would not be useful for this audience. In addition, any changes can

be updated real time and communicated to this larger audience in a more efficient and effective manner.

164.510 Uses and Disclosures requiring an Opportunity for the Individual to Agree or Object: Facility Directory: By participating in a Health Information Exchange, a patient may be a part of a Health Information Exchange directory (no longer just facility focused). There needs to be further thoughts as to what messages should be provided to authorized users of the application (either by role or as provided by the patient) if a individual does elect to participate in the Health Information Exchange but decides to limit the information that may be viewed or limit who may view their information. In addition, once a individual consents to participate, are the capabilities to allow for data and/or individual specific restrictions required?

164.528 Accounting of Disclosures of Protected Health Information. For Health Information Exchange (HIE) organizations or organizations that provide similar services (e.g. organizations that offer a Personal Health Record or similar product) , an accounting of disclosures including those disclosures for treatment, payment and healthcare operations, must be made available to the patient. This allows for the transparency of all disclosures for information contained within the HIE. Again, this allows the patient to become more engaged in their healthcare and encourages participation.

164.524(c)(2) Access of Individuals to Protected Health Information: For individuals that participate in the Health Information Exchange, these participants and/or their Health Information Exchange agent should be able to request that an electronic copy of their information contained by Covered Entities be provided to their Health Information Exchange (HIE) account. All patients have a right to obtain a copy of their health information without data being filtered by the source. This should be adjusted to allow for patients to require that electronic information is either made available to them or their agent for download and/or the option to request a transmission of their information to their own HIE record contained with the HIE within a reasonable timeframe (e.g. day, week). In order to effectively operate as a HIE that allows for consumer controls, this information needs to be provided to the consumer or an agent that is acting on their behalf.

164.506 Uses and Disclosures to Carry Out Treatment, Payment or Healthcare Operations (b) Consent for Uses and Disclosures permitted: The consent to participate in a Health Information Exchange (HIE) should be included; however, further consideration is needed to address privacy vs. patient safety concerns. From a consent perspective, including are three levels of consent:

1. *Consent to allow data to be provided to the HIE agents working on a patient's behalf (within a reasonable timeframe).*
2. *Consent by the individual to provide their health information to their healthcare provider beyond their own access (consumer view).*

3. *Consent to show or mask certain data elements (e.g. sensitive data elements as defined by state laws)*

For item 1, if a consumer decides to not participate or chooses to not participate for a specific time period there may be an information gap in their longitudinal health record, unless there is a provision to require transmission of the missing health information upon participation. For items 2 and 3, is it an acceptable risk to allow the consumer to be able to grant or deny access to either specific providers and/or specific data if it may result in introducing patient safety or diagnosis decision support concerns? In addition, there are different consent/authorization requirements across state lines, most are focused on paper processes, and there is no standard terminology regarding "HIE participation".

3. Business Associates

The CPS workgroup is concerned that an electronic health information exchange environment may lead to an unwieldy amount of contractual relationships in the form of business associate agreements each with their own specific confidentiality, privacy, and security nuances – with limited direct enforcement. The workgroup is seeking comments on the pros and cons of having business associates directly responsible for HIPAA requirements – not through contractual arrangements. If you are a business associate please answer the following questions:

A) **How does you organization ensure compliance with the privacy and security policies of covered entities with whom it contracts, particularly when there are numerous contracts?**
We have established policies and procedures as it relates to privacy and security and work with our third party vendor to assure compliance. As suggested above, there should be an accreditation or certification body that review for a minimum level of HIPAA compliance as it relates to Health Information Exchange efforts and/or any organization that may provide services for such an effort. This will eliminate the need for multiple inspections by organizations participating in these efforts and assist in making organizations comfortable with the practices that are in place at the Health Information Exchange. In addition, this could also be considered a "seal of approval" for the consumer who is interested in monitoring their own healthcare and wants a "trusted source" to provide them with their information. Finally, consumers want to know that their information is being independently monitored and tracked for privacy and security compliance.

B) **How do you handle business associate contracts with large numbers of covered entities including compliance with each covered entity's privacy policies?**

Currently, we are leveraging existing industry Business Associate language and provide those to organizations in which we contract. In addition, we have our own policies and procedures as they relate to HIPAA standards and demonstrate to our participating entities that we adhere to at least HIPAA level standards.

C) **How are business associate agreements negotiated? Do you have a standard contract?**

Negotiated through Legal Counsel - A standard contract is suggested with each participating entity. However, each contract ultimately varies to some degree.

D) **How is the data protection compliance of subcontractors ensured and/or assessed?**
Signed Business Associate contracts are in place.

E) **Do you have subcontractors and how do you handle those agreements?**
See above.

F) **How would direct accountability for meeting relevant HIPAA requirements impact your business?**
In order to be successful, Health Information Exchanges (HIE) need to be held at a minimum to HIPAA standards like other Covered Entities in order to ensure these organizations that privacy and security mechanisms are in place. This is also an important foundation for building trust among healthcare organizations as well as with consumers over time. In the absence of these requirements, resources and time will be wasted with redundant surveys, audits, and discussions surrounding how our organization currently adheres to these standards anyway.

4. General Questions

The CPS workgroup is seeking comment on any of the following additional questions.

A) **What are the implications of having some entities performing similar services covered by federal law (e.g., HIPAA) and others not? For example, a personal health record (PHR) could be offered by a health plan (covered entity) and an independent PHR service provider (non-covered entity).**

i. **How does this impact your competitiveness?**
*All entities that provide HIE services should be on a level playing field and be covered entities. This will allow for more effici*ent contractual completion and *implementation processes across covered entities. Unfair advantage could not be gained by non-covered entities who could potentially under invest in controls, which may result in a breach that impacts the trust and success of all of HIEs in this emerging marketplace.*

ii. **How does this impact your ability to exchange information with others?**
We currently have to undertake complex contract negotiations and operation reviews because we are not a covered entity as defined by HIPAA today. It provides a mechanism for certain stakeholders to significantly slow down their due diligence process to ensure compliance even when recent audits and documentation reviews has already occurred.

iii. **Does contracting with non-covered entities create different levels of accountability and/or enforceability in the exchange of health information?**
Yes – see above comments

B) **Assuming you are not a covered entity, what would be the implications of complying with enforceable confidentiality, privacy, and security requirements at least equivalent to relevant HIPAA principles?**
None for Healthe Mid-America outside of the comments above – we are operating as if we are a covered entity when possible, recognizing that HIEs may very well be re-classified in the not-so-distance future.

C) **Is there a minimum set of confidentiality, privacy, and security protections that you think everyone should follow, if not HIPAA, what?**

Every organization engaged in health care transactions, transmissions and/or storing of health information should be held to privacy and security standards. Overall, the HIPAA privacy and security standards allow for a floor; however, in some instances there may be some differences that must be accounted for such as state laws etc.

[i] Healthe Mid-America is changing its name to **CareEntrust** to better reflect our mission.